木卫四科技
CALLISTOTECHNOLOGY

2024 半年度

汽车漏洞及威胁情报-简报

随着智能汽车技术的快速发展，其安全问题也日益成为行业关注的焦点。2024年上半年的威胁情报分布统计显示，智能汽车领域的安全形势正日趋严峻。

32%
漏洞情报

漏洞情报涉及远程攻击、近场攻击以及本地攻击等

68%
安全事件情报

安全事件情报占据了主要部分，涉及数据泄露、数据篡改、恶意软件攻击、无线网络侵入等

本报告中智能汽车威胁情报的来源多样，每种来源都为我们提供了独特的视角和数据，帮助我们构建一个多维度的威胁情报体系，增强对智能汽车安全风险的认识。

主流的新闻媒介、汽车生态社区发布的智能汽车安全事件的占比高达60%，已经达到了一个值得重视的比例，也反映出公众对智能汽车安全问题的日益关注。

60%
主流的新闻媒介、汽车生态社区

32%
漏洞平台

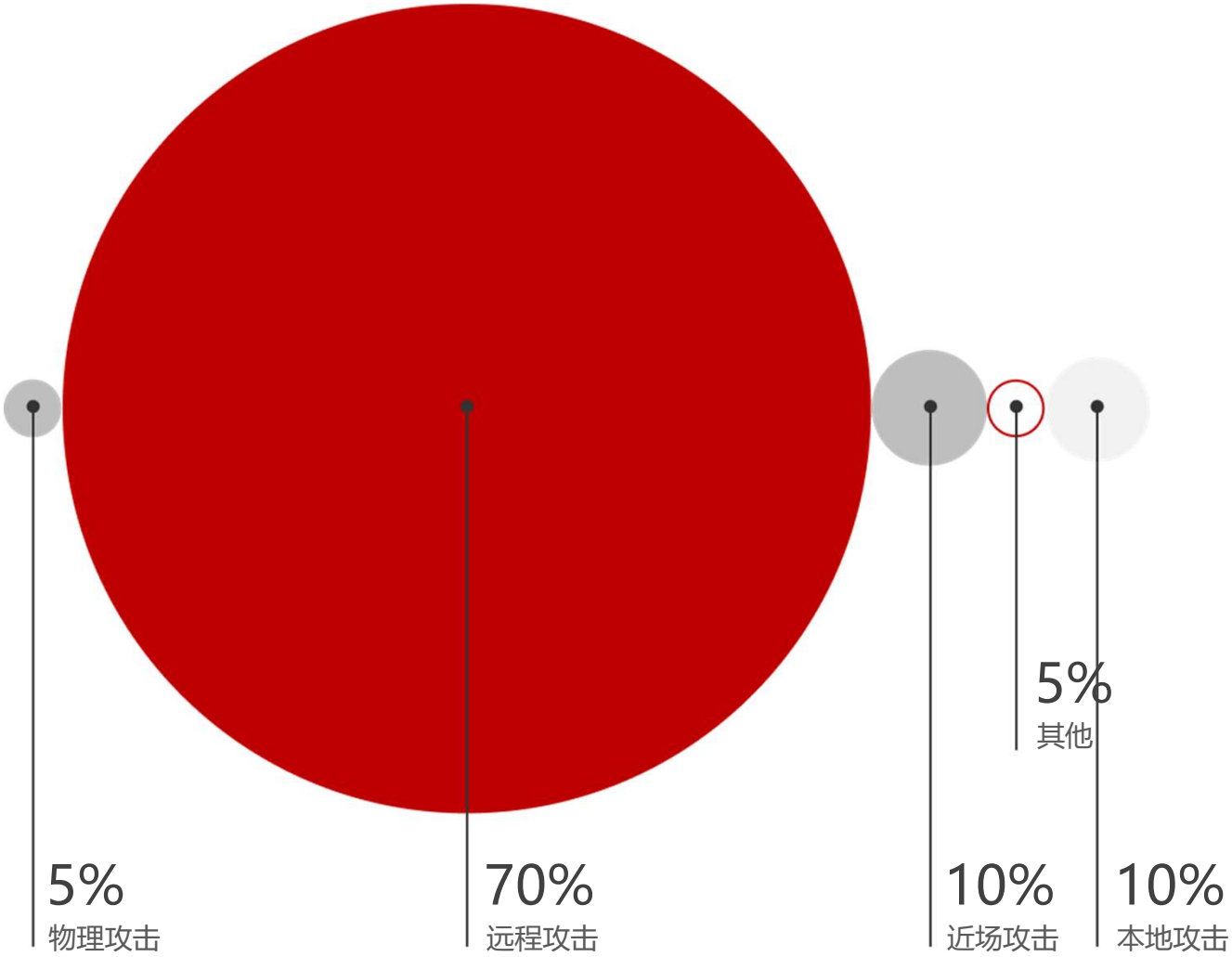
漏洞平台公布的车联网漏洞占比紧跟其次，进一步凸显了加强智能汽车安全防护的紧迫性。

6%
社交媒体

1%
安全博客

1%
安全会议

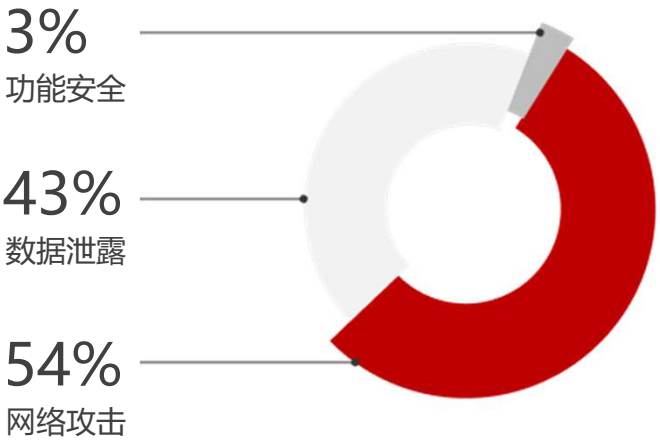
攻击向量分析



2024年上半年，智能汽车面临的攻击向量多种多样，涵盖了远程、近场、本地、物理和其他形式的攻击。深入分析这些攻击向量，有助于理解攻击者的手段和策略，从而制定更有效的防御措施。

事件类型分析

在2024年上半年，智能汽车领域面临的安全事件种类繁多，网络攻击事件、数据泄露事件和功能安全事件各自呈现出独特的威胁特征。根据统计，网络攻击事件的数量占比最多，占所有安全事件的54%。



安全事件

January

- 斯柯达汽车的MIB3信息娱乐系统固件中存在硬编码的UDS服务凭证，暴露了关键的秘密值。这些硬编码凭证，包括密码和加密密钥，用于系统的入站身份验证、与外部组件的出站通信以及内部数据的加密。
- 梅赛德斯-奔驰因员工意外泄露了代码仓库凭证，导致公司内部数据面临严重泄露风险。该凭证为访问公司的GitHub Enterprise Server提供了不受限制的权限，使任何人都能下载公司的私有源代码存储库。

February

- 由于配置错误，宝马开发环境中的Microsoft Azure存储服务器(即“存储桶”)被意外暴露为公共访问。该存储桶包含脚本文件，泄露了Azure容器访问信息、用于访问私有存储桶的密钥及其他云服务的详细信息。
- 日产汽车豪华品牌英菲尼迪美国公司遭遇Mogilevich勒索软件组织攻击，导致22GB包含车辆识别号、客户姓名、地址、电子邮件和密码的敏感数据泄露。

March

- 安全研究人员发现了一种通过伪造特斯拉官方WiFi和登录界面进行网络钓鱼的攻击方法，诱骗车主输入账号凭证，进而激活手机钥匙并完全控制车辆。
- 科罗拉多州立大学研究人员发现美国商用卡车的电子记录设备(ELDs)存在严重漏洞，可被攻击者通过蓝牙或Wi-Fi控制并传播蠕虫攻击。

April

- 西班牙充电设备公司的电动汽车充电器存在未授权访问的漏洞，允许未授权的攻击者通过网络接口访问敏感信息。
- 本田越南公司的数据库在黑客论坛泄露，泄露的信息包含客户ID号、电话号码、车辆类型和购买详情等敏感信息。

May

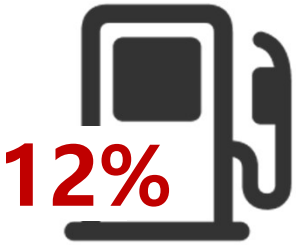
- 安全研究人员发现Tesla Model 3 存在网关固件签名验证绕过漏洞，此漏洞允许网络相邻攻击者在车辆上执行任意代码。
- 日产北美公司近期遭遇数据泄露事件，导致超过53,000名现任和前任员工的个人信息（包括姓名和社会保障号码）被曝光。
- 意大利电动汽车充电设备默认凭证的安全漏洞，攻击者利用此漏洞可能导致设备禁用、付款绕过或支付数据访问。

June

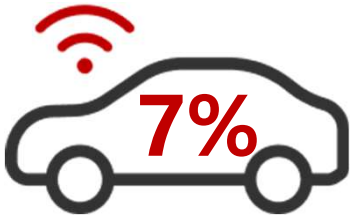
- 安全研究员发现施耐德电气的充电桩存在资源暴露漏洞，该漏洞允许攻击者无需身份验证通过远程端口扫描和指纹识别执行拒绝服务攻击。
- CDK Global遭遇网络攻击，导致约15,000家美国汽车经销商的销售运营被迫暂停，包括通用汽车经销商和拥有数百家经销店的Group 1 Automotive。
- 某车辆管理系统存在严重的安全漏洞，此漏洞可能被利用进行远程攻击。

智能场景威胁覆盖度

智能座舱 发生的威胁风险主要集中在**信息娱乐系统和用户接口**

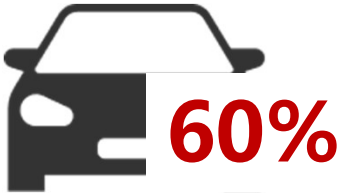


智能充电服务 发生的威胁风险主要集中在**充电站和充电通信协议**



智能控车 发生的威胁风险主要集中在**车辆远程控制和驾驶辅助系统**

智能驾驶 发生的威胁风险主要集中在**自动驾驶系统**



其他场景 发生的威胁风险主要集中在**TSP服务和隐私数据**

影响资产分析

智能汽车领域的安全事件对多种关键资产造成了广泛而深远的影响。这些资产包括敏感数据、充电服务、TSP服务（远程服务平台）、智能座舱等多个重要领域。以下是对不同资产受影响情况的详细分析。

随着智能汽车的数据收集和车载功能不断扩展，敏感数据和安全问题变得尤为严峻。

敏感数据的安全问题尤为突出，其在所有安全事件中的占比高达47%。这些事件通常包括数据泄露和数据篡改等风险，对个人隐私和企业机密构成严重威胁。紧随其后的是TSP服务和智能座舱系统也成为网络攻击者的主要目标。

47% 敏感数据

14% TSP服务

13% 智能座舱

智能电动汽车的普及使得充电基础设施的安全性至关重要。

14%

充电服务 攻击者通过入侵充电站控制系统或利用充电通信协议漏洞，影响车辆充电安全和充电效率。

智能汽车领域的安全事件对多种关键资产造成了严重而深远的影响。这些资产包括智能钥匙、车载设备、车载网络、ADAS系统等。

6%

ADAS系统

攻击者通过入侵ADAS系统，获取控制权限或篡改系统数据，影响自动驾驶功能，导致驾驶风险。

3%

智能钥匙

作为车辆访问和启动的核心组件，智能钥匙在安全事件中可能面临克隆和非法访问的风险，威胁车辆的物理安全。

2%

车载网络

车载网络是连接车辆各电子控制单元的纽带，一旦遭受网络攻击，可能导致车辆控制失效，甚至引发安全事故。

1%

车载设备

车载信息系统、导航设备、娱乐系统等车载设备在遭受攻击时，不仅可能泄露用户数据，还可能影响车辆的正常功能和驾驶体验。

关于木卫四

木卫四（北京）科技有限公司是由全球首批专注于汽车网络安全的技术专家创立、由全球知名机构投资、具备多项自主知识产权的国家高新技术企业。

木卫四正为全球智能汽车领域、自动驾驶和高级驾驶辅助系统的领军企业提供强有力的网络安全支持。客户包括但不限于宝马中国、福特中国、赛力斯、奇瑞、上汽、广汽、蔚来、合众等汽车行业佼佼者。木卫四的发展得益于众多生态伙伴的大力支持，包括华为云、亚马逊云、百度、腾讯云、微软云、地平线、天准科技、艾拉比、德勤、普华永道等知名企业。

关于木卫四S3-VTI

S3-VTI 木卫四汽车威胁情报平台专为车企及供应链系统量身打造，提供全面的汽车专用情报、事件跟踪、车辆漏洞检测、威胁影响分析及缓解措施建议。作为国内首个专为智能网联汽车生态系统设计的威胁情报及漏洞管理解决方案，S3-VTI 平台致力于收集、分析和发布汽车行业的威胁情报，面向车厂、一级供应商（Tier 1）、二级供应商（Tier 2）及网联汽车服务提供商等多个细分市场，提供定制化的汽车威胁情报服务。

木卫四（北京）科技有限公司

官网：
https://www.callisto-auto.com

联系邮箱：
contact@callisto-auto.com